デスクトップ マネジメントについて
Business PC

デスクトップ マネジメントについて

Business PC

初版 2007 年 7 月

製品番号：451272-291

このガイドについて

このガイドでは、一部のモデルにプリインストールされているセキュリティ機能とマネジメント機能の概念および使用手順について説明します。

⚠ **警告！** その指示に従わないと、人体への傷害や生命の危険を引き起こすおそれがあるという警告事項を表します。

△ **注意：** その指示に従わないと、装置の損傷やデータの損失を引き起こすおそれがあるという注意事項を表します。

注記： 重要な補足情報です。

目次

1 デスクトップ マネジメントの概要

HP Client Management Solutions は、ネットワーク環境にあるデスクトップ、ワークステーション、およびノートブック コンピュータの管理と制御の分野で、標準のソリューションを提供しています。HP はデスクトップ マネジメントのパイオニアとして 1995 年に、デスクトップを完全に管理できる業界初のパーソナル コンピュータを世に送り出しました。HP はマネジメント機能の特許を取得しています。以来、デスクトップ、ワークステーション、およびノートブック コンピュータの効果的な導入、設定、および管理に必要な標準化とインフラストラクチャの開発において業界全体の取り組みをリードしてきました。HP は独自の管理ソフトウェアを開発し、業界トップ クラスの管理ソフトウェア ソリューション提供企業との提携関係により、これらの企業の製品と HP Client Management Solutions の互換性を確保しています。HP Client Management Solutions は、ライフサイクル全体を通した PC の所有および管理の総費用削減に役立つソリューションを提供する幅広い取り組みの中でも重要な位置を占めるものです。

デスクトップ マネジメントの主要な機能と特長は、次のとおりです。

- 出荷時設定の変更
- リモート システム インストール
- ソフトウェア アップデートおよびマネジメント機能
- ROM フラッシュ
- ハードウェア オプションの構成
- 資産情報管理機能およびセキュリティ機能
- 障害通知および復旧機能

注記： このガイドで説明される機能のサポートについては、機種またはソフトウェアのバージョンにより異なることがあります。

2 出荷時設定の変更

お使いのコンピュータには、システム ソフトウェア イメージがプリインストールされています。ソフトウェアの設定手順を簡単に済ませると、すぐにコンピュータを使用できます。

プリインストールされたソフトウェア イメージの代わりにカスタマイズされたシステム ソフトウェアおよびアプリケーション ソフトウェアを使うこともできます。カスタマイズされたソフトウェア イメージを展開するには、いくつかの方法があります。

- プリインストールされたソフトウェア イメージを展開した後、追加するアプリケーションをインストールする
- HP OpenView Client Configuration Manager（Windows Vista では現在使用不可）、HP OpenView PC Configuration Management Solution（Radia テクノロジ ベース）（Windows Vista では現在使用不可）、Altiris Deployment Solution などのソフトウェア導入用ツールを使用して、プリインストールされたソフトウェア イメージをカスタマイズされたソフトウェア イメージで置き換える
- ディスク複製手順を使用して、ハードディスク ドライブの内容を別のハードディスクにコピーする

最適なコンピュータ環境の構築方法は、お使いの情報技術環境や作業内容によって異なります。HP ライフサイクル サービスに関する弊社のホームページ（http://h20219.www2.hp.com/services/cache/80906-0-0-225-121.html（英語サイト））には、お使いの環境に適したコンピュータの導入方法の選択に役立つ情報が掲載されています。

Restore Plus! CD、ROM からのセットアップ、および ACPI ハードウェアにより、システム ソフトウェアのリストア、コンフィギュレーション マネジメント機能、トラブルシューティング、および省電力機能を利用することができます。

注記： Restore Plus! CD の作成について詳しくは、「10 ページの 「HP Backup and Recovery Manager」」を参照してください。

HP OpenView Agent

注記： HP OpenView Agent は、Windows Vista では現在使用できません。

HP OpenView Client Configuration Manager および HP OpenView PC Configuration Management Solution の両方で使用される管理エージェントは、コンピュータにプリロードされています。インストールすると、HP OpenView 管理コンソールとの通信が可能になります。

HP OpenView Agent をインストールするには、以下の手順で操作します。

1. **[スタート]**をクリックします。
2. **[すべてのプログラム]**をクリックします。
3. **[HP Manageability]**をクリックします。
4. **[Radia Management Agent Readme]**をクリックします。
5. Readme ファイルに記載されている手順を確認し、それに沿って HP OpenView Agent をインストールします。

HP OpenView Agent は、HP OpenView PC Configuration Management Solution のすべてを有効にするための主要なインフラストラクチャ コンポーネントです。HP OpenView PC Configuration Management Solution の実行に必要なその他のインフラストラクチャ コンポーネントについて詳しくは、http://h20229.www2.hp.com/solutions/ascm/index.html（英語サイト）を参照してください。

Altiris Deployment Solution Agent

このプログラムは、コンピュータにプリロードされています。このプログラムをインストールすると、管理者の Deployment Solution コンソールとの通信が可能になります。

Altiris Deployment Solution Agent をインストールするには、以下の手順で操作します。

1. **[スタート]**をクリックします。
2. **[すべてのプログラム]**をクリックします。
3. Windows Vista の場合は、**[Install Altiris DAgent]**（★Altiris Dagent のインストール★）をクリックします。

   Windows XP の場合は、**[Install Altiris AClient]**（★Altiris AClient のインストール★）をクリックします。
4. 画面の説明に沿って、Altiris クライアントのセットアップと設定を行います。

Altiris Deployment Solution Agent は、HP Client Foundation Suite および Client Premium Suite を有効にするための主要なインフラストラクチャ コンポーネントです。HP Client Foundation Suite および Client Premium Suite の実行に必要なその他のインフラストラクチャ コンポーネントについて詳しくは、http://www.hp.com/go/easydeploy（英語サイト）を参照してください。

3　リモート システム インストール

Preboot Execution Environment（PXE）を起動すれば、リモート システム インストールを使用してネットワーク サーバからソフトウェアやコンフィギュレーション情報（コンピュータの設定情報）を取り出し、コンピュータを起動してセットアップすることができます。リモート システム インストールの機能は、通常、システム セットアップやコンフィギュレーションのためのツールとして使用しますが、次のような場合にも使用できます。

- ハードディスク ドライブをフォーマットするとき
- 1 台以上の新しいコンピュータにソフトウェア イメージを導入するとき
- フラッシュ ROM を使用してシステム BIOS をリモートでアップデートするとき（「15 ページの 「リモート ROM フラッシュ機能」」を参照）
- システム BIOS を設定するとき

リモート システム インストールを起動するには、起動時に表示される HP ロゴの画面の右下隅に**[F12 = Network Service Boot]**と表示されたら、すぐに F12 キーを押します。画面のメッセージに従って、リモート システム インストールを起動します。初期設定の起動順序は BIOS のコンフィギュレーションですが、常に PXE を起動するように変更できます。

4 ソフトウェアのアップデートと管理

HP では、デスクトップ コンピュータ、ワークステーション、およびノートブック コンピュータのソフトウェアを管理し、アップデートするための以下のツールを提供しています。

- HP Client Management Interface
- HP System Software Manager
- HP Client Manager
- HP ProtectTools セキュリティ マネージャ
- HP Client Premium Suite
- HP Client Foundation Suite
- HP OpenView Client Configuration Manager（Windows Vista では現在使用不可）
- HP OpenView PC Configuration Management Solution（Windows Vista では現在使用不可）
- HP Client Catalog for SMS
- HP Backup and Recovery Manager
- Active Management Technology 対応の Intel vPro 搭載コンピュータ
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

IT 部門で使用しているシステム管理ツールに関係なく、ハードウェア アセットとソフトウェア アセットの両方を管理することは、IT コストの削減とビジネスの迅速化にとって重要です。IT 管理者は簡単なスクリプトを作成して目的の管理ソリューションに組み込むことによって、HP Client Management Interface にアクセスできます。

HP Client Management Interface（HP CMI）を使用すると、HP ビジネス コンピュータはユーザが管理する IT 環境とシームレスに統合されます。HP CMI は、HP ビジネス コンピュータと一般的なシステム管理ツール（Microsoft Systems Management Server、IBM Tivoli Software、HP OpenView Operations など）および社内で開発した管理アプリケーションとの統合を簡略化するインタフェースを提供します。HP CMI を使用すると、システム管理ツールとアプリケーションが直接クライアント コンピュータと通信することで、詳細なクライアント インベントリを要求したり、システム状態情報を受信したり、システムの BIOS 設定を管理したりできます。その結果、エージェントやコネクタ ソフトウェアが統合を行う必要が少なくなります。

HP Client Management Interface は、Microsoft Windows Management Interface（MS WMI）、Web-Based Enterprise Management（WBEM）、System Management BIOS（SMBIOS）、および Advanced Configuration and Power Interface（ACPI）などの業界標準に準拠しています。HP CMI は、HP Client Management Solutions で使用される基礎テクノロジです。HP CMI を使用すると、HP クライアント コンピュータの管理方法を柔軟に選択できるようになります。

HP Client Management Interface をシステム管理ソフトウェアと併用すると、次のことが可能になります。

- 詳細なクライアント インベントリ情報の要求：プロセッサ、ハードディスク ドライブ、メモリ、BIOS、ドライバなどに関する詳細情報を取得します。センサ情報（ファンの速さ、電圧、温度など）も含まれます。
- システム状態情報の受信：システム管理コンソール、アプリケーション、またはローカル クライアント コンピュータに対する幅広いクライアント ハードウェア警告（適正温度の超過、ファンの停止、ハードウェア構成の変更など）の送信を登録します。警告は、ハードウェア イベントによってトリガされたときにリアルタイムで送信されます。
- システム BIOS 設定の管理：任意のまたはすべてのクライアント システム上のシステム管理コンソールから、各マシンに移動することなくリモートで F10 機能（BIOS パスワードおよびコンピュータのブート順序の設定や変更など）を実行します。

HP Client Management Interface について詳しくは、http://www.hp.com/go/hpcmi/（英語サイト）を参照してください。

HP System Software Manager

HP System Software Manager（SSM）は、ネットワーク上にある HP Business PC のデバイス ドライバおよび BIOS アップデートのリモート展開を自動化するための、無料のユーティリティです。SSM を実行すると、各ネットワーク クライアント システムにインストールされているドライバおよび BIOS のリビジョン レベルが（ユーザとの対話なしに）自動的に確認され、このインベントリと、すでにテストされ、中央のファイル格納ディレクトリに格納されているシステム ソフトウェアの SoftPaq が比較されます。SSM では次に、ネットワーク PC 上の古いリビジョンのシステム ソフトウェアが、ファイル格納ディレクトリで使用可能な最新のレベルに自動的にアップデートされます。SSM では SoftPaq アップデートが正しいクライアント システム モデルにだけ配布されるため、管理者は確実かつ効率的に、SSM を使用してシステム ソフトウェアを最新版に維持できます。

System Software Manager は、HP OpenView PC Configuration Management Solution（Windows Vista では現在使用不可）、Altiris HP Client Manager、Microsoft Systems Management Server（SMS）などのエンタープライズ ソフトウェア配布ツールと統合されています。SSM を使用すると、SSM 形式にパッケージ化された、顧客が作成したアップデートや他社製アップデートを配布できます。

SSM は、http://www.hp.com/go/ssm（英語サイト）から無料でダウンロードできます。

注記： Windows Vista BitLocker が有効になっていて、TPM 測定を使用しているシステムでは、BIOS をフラッシュすると、BitLocker がプラットフォーム用に作成した信頼署名が無効になります。そのため、このようなシステムの場合、BitLocker キーを保護するために、SSM では現在リモート ROM フラッシュがサポートされていません。システム BIOS をフラッシュするには、グループ ポリシーで BitLocker を無効にしてください。

BIOS の TPM 測定を使用せずに BitLocker サポートを有効にすると、BitLocker キーが無効になることを防ぐことができます。緊急時にリカバリできるように、BitLocker 証明書をバックアップしておくことをおすすめします。

HP Client Manager

Altiris 社で開発された HP Client Manager は、サポートされているすべての HP Business Desktop PC、ノートブック コンピュータ、およびワークステーション モデルで無料で使用できます。SSM は、HP Client Manager に統合されており、HP クライアント システムのハードウェアの状態を中央から追跡、監視、および管理できるようにします。

HP Client Manager を使用すると、次のことが可能になります。

- CPU、メモリ、ビデオ、セキュリティ設定などの役立つハードウェア情報を取得する
- システム状態を監視して、問題が発生する前に解決できるようにする
- ドライバおよび BIOS アップデートを、各 PC の場所まで移動せずに自動的に取得してインストールする
- BIOS やセキュリティ設定をリモートで設定する
- ハードウェアの問題を迅速に解決するためのプロセスを自動化する

HP Instant Support ツールに統合すると、ハードウェアの問題解決の時間を短縮できます。

- 診断 : HP のデスクトップ、ノートブック、およびワークステーション モデルでレポートをリモートで実行および表示する
- システム状態のスキャン : HP クライアント システムの設置基盤での既知のハードウェア問題をチェックする
- アクティブ チャット : HP カスタマ サポートに問い合わせて問題を解決する
- HP ナレッジベース : 専門的な情報にリンクする
- ハードウェアの問題を迅速に解決するための SoftPaq の自動的な収集および配信プロセス
- HP ProtectTools 内蔵セキュリティ チップを使用したシステムの認識、インベントリ、および初期化
- クライアント システムでシステム状態警告をローカルで表示するオプション
- HP 以外のクライアントの基本インベントリ情報のレポート
- TPM セキュリティ チップのセットアップと設定
- クライアントのバックアップとリカバリの集中スケジュール管理
- Intel AMT の管理用アドオン サポート

HP Client Manager について詳しくは、http://www.hp.com/go/clientmanager（英語サイト）を参照してください。

HP ProtectTools セキュリティ マネージャ

ProtectTools セキュリティ マネージャ ソフトウェアは、コンピュータ本体、ネットワーク、および重要なデータを不正なアクセスから保護するために役立つセキュリティ機能を提供します。以下のモジュールによって、高度なセキュリティ機能が提供されます。

- スマート カード セキュリティ
- Embedded Security for ProtectTools
- BIOS Configuration for ProtectTools
- Credential Manager for ProtectTools

コンピュータで利用可能なモジュールは、モデルによって異なる可能性があります。たとえば、Embedded Security for ProtectTools を使用するには、TPM（Trusted Platform Module）内蔵セキュリティ チップ（一部のモデルのみ）がコンピュータに搭載されている必要があり、また、スマート カード セキュリティを使用するにはオプションのスマート カードおよびリーダーが必要です。

ProtectTools モジュールは、プリインストールまたはプリロードされている場合と、HP の Web サイトから購入できる場合があります。詳しくは、http://www.hp.com/products/security/（英語サイト）を参照してください。

HP Client Premium Suite

HP Client Premium Suite（HP CPS）は、単一の Web ベースの管理コンソールからクライアント ハードウェアおよびソフトウェアの全ライフサイクルを管理する必要がある組織向けに設計されています。次のものが含まれています。

- HP Client Manager
- HP Systems Insight Manager Connector
- HP OpenView Connector（Windows Vista では現在使用不可）
- Altiris Client Manager Suite - Level 1
- Altiris Connector Solution
- Altiris Local Recovery Pro
- Altiris AuditExpress

HP Client Premium Suite について詳しくは、http://www.hp.com/go/easydeploy/（英語サイト）を参照してください。

HP Client Foundation Suite

HP Client Foundation Suite（HP CFS）は、重要なクライアント管理機能が必要な組織向けに設計されています。次のものが含まれています。

- HP Client Manager
- HP Systems Insight Manager Connector
- Altiris Migration Suite
- Altiris Local Recovery Pro

HP Client Foundation Suite について詳しくは、http://www.hp.com/go/easydeploy/（英語サイト）を参照してください。

HP OpenView Client Configuration Manager

注記： HP OpenView Client Configuration Manager は、Windows Vista では現在使用できません。

HP OpenView Client Configuration Manager は、Windows XP および HP Thin Client 環境向けの使いやすく、すばやく導入できるハードウェアおよびソフトウェア管理ソリューションであり、将来の要件に対応する強力な基盤を提供します。次の 2 つのバージョンで提供されます。

- Basic Edition は、HP のデスクトップ コンピュータ、ノートブック コンピュータ、およびワークステーションを管理するための無料の製品であり、ハードウェアおよびソフトウェア インベントリ、リモート制御、HP アラート監視、HP BIOS およびドライバ アップデート、HP Protect Tools との統合、Intel AMT に対するアドオン サポートなどの機能を提供します。Basic Edition はまた、HP Thin Client の導入と管理もサポートします。
- 購入が可能な Premium Edition には、Basic Edition で提供されるすべての機能が含まれているほか、Windows の導入と移行、パッチ管理機能、ソフトウェア配布、およびソフトウェア使用率計測が追加されています。

HP Client Configuration Manager では、絶えず変化する大規模で、種類の異なる IT 環境を自動的に管理するための、HP OpenView PC Configuration Management Solution（Radia テクノロジ ベース）への移行パスが提供されます。

HP OpenView Client Configuration Manager について詳しくは、http://www.managementsoftware.hp.com/products/ccm/index.html（英語サイト）を参照してください。

HP OpenView PC Configuration Management Solution

注記：　HP OpenView PC Configuration Management Solution は、Windows Vista では現在使用できません。

HP OpenView PC Configuration Management Solution は、管理者が、種類の異なるクライアント プラットフォームにわたってソフトウェアとコンテンツのインベントリ管理、展開、パッチの適用、および連続的な管理を行うことのできる、ポリシー ベースのソリューションです。HP OpenView PC Configuration Management Solution を使用すると、IT 技術者は次のことが可能になります。

- 検出、導入から、移行や運用停止までの継続的な管理といった、ライフサイクル管理プロセス全体を自動化する。
- ソフトウェア スタック全体（オペレーティング システム、アプリケーション、パッチ、設定、およびコンテンツ）を自動的に展開し、望ましい状態になるように継続的に管理する。
- 異種またはスタンドアロン インフラストラクチャ内にある、デスクトップ コンピュータ、ワークステーション、ノートブック コンピュータを含む、ほぼ任意のデバイスのソフトウェアを管理する。
- ほとんどのオペレーティング システム上でソフトウェアを管理する。

継続的な構成管理により、HP のお客様からは、IT コストの大幅な削減、ソフトウェアやコンテンツを市場に投入するまでの時間の短縮、およびユーザの生産性と満足度の向上が報告されています。

HP OpenView PC Configuration Management Solution について詳しくは、http://h20229.www2.hp.com/solutions/ascm/index.html（英語サイト）を参照してください。

HP Client Catalog for SMS

更新管理は、個々の PC から企業のデータセンタに至るあらゆるコンピュータのメンテナンスのための重要な機能です。更新があるかどうかを特定し、必要な更新をタイミングよく自動的に配信できることは、管理する組織のセキュリティと生産性の維持に役立ちます。HP では、Microsoft System Management Server 管理インフラストラクチャ内の HP システムの更新を効率化する機能を提供しています。HP Client Catalog for SMS には、デスクトップ、モバイル、ワークステーションの各プラットフォーム用にソフトウェア ドライバとパッチ情報が用意されています。プラットフォーム別の詳細情報は、HP Client Catalog for SMS によって企業内の該当のクライアント システムに配信されます。SMS 2003 R2 と Inventory Tool for Custom Updates を使用すると、この詳細情報に基づいて組織内で HP ソフトウェアの更新をすばやく簡単に統合して配信できます。

HP Client Catalog for SMS について詳しくは、http://www/hp/com/go/easydeploy/（英語サイト）を参照してください。

HP Backup and Recovery Manager

HP Backup and Recovery Manager は、使いやすく多目的に利用できるアプリケーションであり、コンピュータのメイン ハードディスク ドライブのバックアップおよび回復を可能にします。HP Backup and Recovery Manager は Windows で動作し、Windows、すべてのアプリケーション、およびすべてのデータ ファイルのバックアップを作成します。バックアップは、指定の間隔で自動的に実行されるようにスケジュール設定することも、手動で開始することもできます。通常のバックアップとは別に重要なファイルのアーカイブを作成できます。

HP Backup and Recovery Manager は、ハードディスク ドライブのリカバリ パーティションにプリインストールされていて、以下の機能を持ちます。

- リカバリ ポイントを作成して、システム全体を段階的にバックアップする。
- 単一のアーカイブにシステム全体をバックアップする。
- 個別のファイルおよびフォルダをバックアップする。

リカバリ ポイントおよびファイルのバックアップは CD または DVD にコピーできますが、システム全体のバックアップはネットワークまたはセカンダリ ハードディスクにコピーできます。

コンピュータを使用する前に、今すぐリカバリ ディスク セットを作成して、リカバリ ポイントの定期的な自動バックアップのスケジュールを設定することを強くおすすめします。

リカバリ ディスク セットを作成するには、以下の手順で操作します。

1. **[スタート]→[すべてのプログラム]→[HP Backup and Recovery]→[HP Backup and Recovery Manager]**の順にクリックして Backup and Recovery Wizard を起動し、**[次へ]**をクリックします。
2. **[Create a set of recovery discs (Recommended)]**（★リカバリ ディスク セットを作成する（推奨）★）を選択し、**[次へ]**をクリックします。
3. ウィザードの説明に沿って操作します。

HP Backup and Recovery Manager には、基本的な 2 つのリカバリ方法があります。1 つは、Windows 上のファイルやフォルダのリカバリです。もう 1 つは、コンピュータのリカバリです。これには、リカバリ パーティションまたはリカバリ ディスク セットからの再起動が必要です。リカバリ パーティションから再起動するには、起動時に**[Press f11 for Emergency Recovery]**（緊急リカバリには f11 キーを押してください）というメッセージが表示されたら、f11 キーを押します。

HP Backup and Recovery Manager について詳しくは、**[スタート]→[HP Backup and Recovery]→[HP Backup and Recovery Manager マニュアル]**の順に選択して、『HP Backup and Recovery Manager ユーザ ガイド』を参照してください。

注記：　リカバリ ディスク セットが必要になった場合は、サポート窓口にお問い合わせください。お問い合わせ先の電話番号については、日本では『サービスおよびサポートを受けるには』の小冊子を参照して、日本以外の国や地域では次の Web サイトにアクセスして地域を選択して確認してください。

http://welcome.hp.com/country/us/en/wwcontact_us.html

Active Management Technology 対応の Intel vPro 搭載コンピュータ

Intel Active Management Technology（AMT）を使用すると、ネットワークに接続したコンピュータ アセットの検出、修復、および保護を適切に行うことができます。AMT によって、システムがオンかオフか、またはオペレーティング システムが停止していないかどうかを管理できます。

Intel vPro の機能には次のものが含まれます。

- ハードウェア インベントリ情報
- 警告
- 電源管理：電源のオンとオフ、再起動
- リモートでの診断および修復
  - Serial-over-LAN：ブート フェーズ中のリモート PC のコンソール制御が可能
  - IDE リダイレクト：リモートのブート ドライブ、ディスク、または ISO イメージからシステムのブートが可能
- ハードウェア ベースの隔離とリカバリ：ウィルスのような動作が検出された場合に、コンピュータ ネットワークへのアクセスを制限または切断

注記：　Intel vPro テクノロジの概要については、http://www.intel.com/jp/vpro/を参照してください。

Intel vPro テクノロジに関する HP 固有の情報については、http://www.hp.com/support/にあるホワイト ペーパーを参照してください。国と言語を選択してから**[サポート&問題解決情報を表示する]**を選択し、コンピュータのモデル番号を入力して Enter キーを押します。**[Resources for my selected product]**（選択した製品向けリソース）カテゴリで、**[Manuals (guides, supplements, addendums, etc)]**（マニュアル（ガイド、補足、付録など））をクリックします。**[Quick jump to manuals by category]**（カテゴリ別のマニュアルへのクイック ジャンプ）で、**[White papers]**（ホワイト ペーパー）をクリックします

Intel vPro 搭載のコンピュータでは、以下の管理機能を使用できます。

- AMT
- ASF
- 仮想化技術（VT）

ASF と AMT は同時に設定できませんが、どちらもサポートされます。

AMT または ASF の Intel vPro システムを設定するには、以下の手順で操作します。

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[終了オプション]**（または**[シャットダウン]**）→**[再起動]**の順に選択します。
2. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに Ctrl ＋ P ホットキーを押します。

   注記：　適切なタイミングで Ctrl ＋ P キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 Ctrl ＋ P キーを押します。

このホットキーで、Intel Management Engine BIOS Execution（MEBx）セットアップ ユーティリティが起動します。このユーティリティを使用すると、管理機能のさまざまな設定を行うことができます。構成オプションには、次のものが含まれます。

- ME プラットフォームの構成
  - ME Platform State Control（ME プラットフォームの状態制御）：管理エンジンを有効/無効にします
  - ME Firmware Local Update（ME ファームウェアのローカル アップデート）：ファームウェア アップデートの管理をローカルで有効/無効にします
  - LAN Controller（LAN コントローラ）：統合ネットワーク コントローラを有効/無効にします
  - ME Features Control（ME の機能制御）：AMT または ASF を有効にするか、両方を無効にします
  - ME Power Control（ME の電源制御）：管理エンジンの電源ポリシーを設定します
- Intel AMT の構成
  - Change AMT Password（AMT パスワードの変更）：AMT の構成に必要です（パスワードの初期値は**[admin]**）
  - Host Name（ホスト名）：管理者はクライアントに名前を割り当てることができます
  - TCP/IP：管理者は IP アドレスを割り当てたり、DHCP を有効にしたりできます
  - Provisioning Server（プロビジョニング サーバ）：管理者はプロビジョニング サーバの IP アドレスを割り当てることができます
  - Provision Model（プロビジョニング モデル）：管理者はエンタープライズ モードと SMB モードのどちらかで構成できます
  - Set PID and PPS（PID と PPS の設定）：管理者はプレプロビジョニング キー（HP のホワイト ペーパー『Intel vPro Provisioning』（英語版）を参照）を指定できます
  - Un-Provision（プロビジョニング解除）：管理者は AMT 構成を出荷時の設定に戻すことができます
  - VLAN：管理者は LAN の仮想化サポートを有効にできます
  - SOL/IDE-R：管理者はリモートのブートおよびコントロール セッションを有効にできます
- MEBx パスワードの変更（このパスワードを変更することを強くおすすめします。パスワードの初期値は**[admin]**です）

リモートで AMT システムを管理するには、管理者は AMT をサポートするリモート コンソールを使用する必要があります。エンタープライズ管理コンソールは、HP OpenView（Windows Vista では現在使用不可）、Altiris、Microsoft SMS などのサプライヤから入手できます。SMB モードでは、Web ブラウザ インタフェースがクライアントで提供されます。この機能にアクセスするには、ネットワーク上にある他の任意のシステムからブラウザを開き、「http://host_name:16992」と入力します。host_name はシステムに割り当てられた名前です。また、ホスト名の位置に IP アドレスを使用することもできます。

HP Proactive Change Notification

Proactive Change Notification プログラムは、Subscriber's Choice の Web サイトを利用して、以下のことを事前にかつ自動的に行います。

- ほとんどの企業向け HP 製コンピュータおよびサーバでハードウェアおよびソフトウェアの変更があった場合に、最も早くて 60 日前に電子メールで Proactive Change Notification（PCN）を送信する
- ほとんどの企業向け HP 製コンピュータおよびサーバについての Customer Bulletins、Customer Advisories、Customer Notes、Security Bulletins、および Driver alerts を含んだ電子メールを送信する

特定の IT 環境に該当する情報のみを受け取るようにするため、ユーザ専用のプロファイルを作成します。Proactive Change Notification プログラムの詳細およびカスタム プロファイルの作成については、http://h30046.www3.hp.com/subhub.php（英語サイト）を参照してください。

Subscriber's Choice

Subscriber's Choice は HP のクライアントベースのサービスです。

ユーザのプロファイルを基に、製品を使用する際のヒント、特集記事、およびドライバやサポートに関する警告や通知を提供します。

Subscriber's Choice Driver and Support Alerts/Notifications では、購読するようプロファイルに設定した情報が閲覧および入手可能になると、電子メールで通知します。Subscriber's Choice の詳細およびカスタム プログラムの作成については、http://h30046.www3.hp.com/subhub.php（英語サイト）を参照してください。

廃止されたソリューション

Altiris Local Recovery と Dantz Retrospect の 2 つのソフトウェア パッケージは、今後 HP のビジネス デスクトップ、ノートブック コンピュータ、ワークステーションには搭載されません。2006 年から新しく発売されるビジネス デスクトップ、ノートブック コンピュータ、およびワークステーションには、HP Backup and Recovery Manager が搭載されます。

5 ROM フラッシュ機能

お使いのコンピュータでは、オペレーティング システムとの情報のやりとりなどを行う基本入出力システム（BIOS）がプログラム可能なフラッシュ ROM（読み取り専用メモリ）に記憶されています。コンピュータ セットアップ（F10）ユーティリティでセットアップ パスワードを設定しておけば、ROM の不用意な更新や上書きを防止できます。これは、コンピュータの動作の整合性を確保するために重要です。BIOS のアップグレードが必要な場合は、http://www.hp.com/support/files（英語サイト）の HP ドライバとサポートのページから最新の BIOS イメージをダウンロードできます。

△ **注意：** ROM を最大限に保護するために、必ずセットアップ パスワードを設定してください。セットアップ パスワードによって、ROM の不正なアップグレードを防止できます。System Software Manager を使用すると、システム管理者が、複数のコンピュータに同時にセットアップ パスワードを設定することができます。詳しくは、http://www.hp.com/go/ssm/（英語サイト）を参照してください。

リモート ROM フラッシュ機能

リモート ROM フラッシュ機能を利用すれば、システム管理者は、ネットワーク管理端末からリモートでコンピュータの BIOS を安全に書き換えることができます。複数の HP のコンピュータに対してこのような作業をリモートで行うことができるので、ネットワーク上のコンピュータの BIOS を適切にアップグレードすることができます。また、生産性を向上させ、少ない費用で管理できます。

注記： Windows Vista BitLocker が有効になっていて、TPM 測定を使用しているシステムでは、BIOS をフラッシュすると、BitLocker がプラットフォーム用に作成した信頼署名が無効になります。そのため、このようなシステムの場合、BitLocker キーを保護するために、SSM では現在リモート ROM フラッシュがサポートされていません。システム BIOS をフラッシュするには、グループ ポリシーで BitLocker を無効にしてください。

リモート ROM フラッシュを使用するには、リモート ウェイク アップ機能を使って、お使いのコンピュータの電源を入れておくか、再起動しておく必要があります。

リモート ROM フラッシュについて詳しくは、http://www.hp.com/go/ssm/.

HPQFlash

HPQFlash ユーティリティは、Windows オペレーティング システムで個別のコンピュータ上でシステム BIOS のアップデートや復元を行う場合に使用します。

HPQFlash について詳しくは、http://www.hp.com/support/files/（英語サイト）で画面の説明に沿ってコンピュータのモデル番号を入力してください。

6 Boot Block Emergency Recovery Mode

Boot Block Emergency Recovery Mode によって、ROM フラッシュに失敗した場合も、システム ROM を復旧またはアップグレードすることができます。たとえば、BIOS のアップグレード中に電源の障害が発生すると、ROM フラッシュは完了しないまま終了します。これにより、システム BIOS が使用不可能になります。Boot Block は、ROM フラッシュの際にも更新されない領域に収められており、コンピュータの電源投入時に有効なシステム BIOS イメージをチェックするコードが含まれています。

- システム BIOS イメージが有効な場合は、コンピュータは通常の方法で起動します。
- システム BIOS イメージが有効でない場合は、Boot Block BIOS によって、BIOS イメージ ファイル用のリムーバブル メディアを検索するための十分なサポートが提供されます。適切な BIOS イメージ ファイルが見つかると、そのファイルが ROM に自動的にフラッシュされます。

無効なシステム BIOS イメージが検出されると、システム電源ランプが 8 回赤く点滅します（1 秒間に 1 回の点滅）。同時に、スピーカからビープ音が 8 回鳴ります。システム ROM の中の、ビデオ オプション ROM イメージが含まれている部分が壊れていなければ、画面に**[Boot Block Emergency Recovery Mode]**と表示されます。

Boot Block Emergency Recovery Mode になったら、以下のように操作して、システム BIOS を復旧（アップグレード）してください。

1. コンピュータの電源を切ります。
2. ルート ディレクトリに目的の BIOS イメージ ファイルが含まれている CD または USB フラッシュ デバイスを挿入します。

   注記： このメディアは、FAT12、FAT16、または FAT32 ファイル システムでフォーマットされている必要があります。

3. コンピュータの電源を入れます。

   適切な BIOS イメージ ファイルが見つからない場合は、BIOS イメージ ファイルが含まれているメディアを挿入するよう指示されます。

   システム BIOS の復旧またはアップグレードが正常に完了すると、システムによって電源が自動的に切られます。

4. BIOS のアップグレードに使用したリムーバブル メディアを取り出します。
5. 電源を入れて、コンピュータを起動しなおします。

注記： BIOS イメージ ファイルが含まれている CD がオプティカル ドライブに挿入されていると、BitLocker によって Windows Vista はブートできなくなります。BitLocker が有効になっている場合は、Windows Vista を起動する前に、この CD を取り出してください。

7 リプリケート セットアップ機能

以下のリプリケート セットアップ機能を使用すれば、管理者がコンピュータの設定情報（コンフィギュレーション情報）を他の同じモデルのコンピュータに簡単にコピーすることができます。この機能によって、複数のコンピュータに同じ設定を行う時間を短縮することができます。

注記：　これらの手順を行うには、ディスケット ドライブ、または HP USB メモリなどのサポートされる USB フラッシュ メディア デバイスが必要です。

1 台のコンピュータへのコピー

注意：　設定情報はモデルにより異なります。コピー元とコピー先のコンピュータが別のモデルの場合、ファイル システムが破損する恐れがあります。たとえば、dc7xxx シリーズのコンピュータから dx7xxx シリーズのコンピュータに設定情報をコピーしないでください。

1. 設定情報コピー元のコンピュータを選択します。コンピュータの電源を切ります。Microsoft Windows を実行している場合は、**[スタート]**→**[シャットダウン]**（または**[終了オプション]**）→**[シャットダウン]**（または**[電源を切る]**）の順に選択します。
2. 設定情報保存用ディスケットまたは USB フラッシュ メディア デバイスをここで挿入します。
3. コンピュータの電源を入れます。
4. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記：　適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。
5. ディスケットを使用する場合はここで挿入します。
6. **[ファイル]**（File）→**[複製セットアップ]**（Replicated Setup）→**[リムーバブル メディアに保存]**（Save to Removable Media）の順に選択します。画面上のメッセージに従って操作し、設定情報ディスケットまたは USB フラッシュ メディア デバイスを作成します。
7. 設定情報コピー先のコンピュータの電源を切り、設定情報ディスケットまたは USB フラッシュ メディア デバイスを挿入します。
8. 設定情報コピー先のコンピュータの電源を入れます。
9. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。
10. **[ファイル]**→**[複製セットアップ]**→**[システム構成の復元]**（Restore from Removable Media）の順に選択したあと、画面上のメッセージに従って操作します。
11. 設定が完了したら、コンピュータを再起動します。

複数のコンピュータへのコピー

△ **注意：** 設定情報はモデルにより異なります。コピー元とコピー先のコンピュータが別のモデルの場合、ファイル システムが破損する恐れがあります。たとえば、dc7xxx シリーズのコンピュータから dx7xxx シリーズのコンピュータに設定情報をコピーしないでください。

この手順では設定情報ディスケットまたは USB フラッシュ メディア デバイスの作成に少し時間がかかりますが、設定情報をコピー先のコンピュータにコピーする時間は大幅に短縮されます。

注記： この手順を行うため、また起動可能 USB フラッシュ メディア デバイスを作成するためには、起動可能ディスケットが必要です。起動可能ディスケットを作成するために Windows XP を使用できない場合は、1 台のコンピュータへのコピーの手順を実行してください（「17 ページの 「1 台のコンピュータへのコピー」」を参照）。

1. 起動可能ディスケットまたは USB フラッシュ メディア デバイスを作成します。「19 ページの 「サポートされる USB フラッシュ メディア デバイス」」または「20 ページの 「サポートされない USB フラッシュ メディア デバイス」」を参照してください。

   △ **注意：** USB フラッシュ メディア デバイスから起動できないコンピュータもあります。コンピュータ セットアップ（F10）ユーティリティに表示される初期設定の起動順序で、USB デバイスがハードディスク ドライブより前にある場合、そのコンピュータは USB フラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

2. 設定情報コピー元のコンピュータを選択します。コンピュータの電源を切ります。Microsoft Windows を実行している場合は、**[スタート]**→**[シャットダウン]**（または**[終了オプション]**）→**[シャットダウン]**（または**[電源を切る]**）の順に選択します。
3. 設定情報保存用ディスケットまたは USB フラッシュ メディア デバイスをここで挿入します。
4. コンピュータの電源を入れます。
5. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。

6. ディスケットを使用する場合はここで挿入します。
7. **[ファイル]**（File）→**[複製セットアップ]**（Replicated Setup）→**[リムーバブル メディアに保存]**（Save to Removable Media）の順に選択します。画面上のメッセージに従って操作し、設定情報ディスケットまたは USB フラッシュ メディア デバイスを作成します。
8. BIOS Utility for Replicated Setup（リプリケート セットアップ用 BIOS ユーティリティ）をダウンロードして、この中に含まれる repset.exe ファイルを設定情報ディスケットまたは USB フラッシュ メディア デバイスにコピーします。このユーティリティを入手するには、http://welcome.hp.com/country/us/en/support.html（英語サイト）にアクセスし、コンピュータのモデル番号を入力します。
9. 設定情報ディスケットまたは USB フラッシュ メディア デバイス上で、次のコマンドを含む autoexec.bat ファイルを作成します。

   repset.exe

10. 設定情報コピー先のコンピュータの電源を切ります。設定情報ディスケットまたは USB フラッシュ メディア デバイスを挿入し、コンピュータの電源を入れます。設定ユーティリティが自動的に実行されます。
11. 設定が完了したら、コンピュータを再起動します。

起動可能デバイスの作成

サポートされる USB フラッシュ メディア デバイス

サポートされるデバイスには、そのデバイスを簡単な手順で起動可能にするためのイメージがプリインストールされています。HP およびコンパックのすべての USB フラッシュ メディア デバイス、またその他のほとんどの USB フラッシュ メディア デバイスにこのイメージがプリインストールされています。使用している USB フラッシュ メディア デバイスにこのイメージが存在しない場合は、後で説明する手順に従ってください（「20 ページの 「サポートされない USB フラッシュ メディア デバイス」」を参照）。

起動可能な USB フラッシュ メディア デバイスを作成するには、次のものが必要です。

- 対応する USB フラッシュ メディア デバイス
- FDISK および SYS プログラムが格納された、起動可能な DOS ディスケット（SYS がない場合は FORMAT を使用できますが、USB メモリ上のファイルがすべて失われます）
- USB フラッシュ メディア デバイスから起動可能なコンピュータ

△ **注意：** 一部の古いコンピュータでは、USB フラッシュ メディア デバイスから起動できない場合があります。コンピュータ セットアップ（F10）ユーティリティに表示される初期設定の起動順序で、USB デバイスがハードディスク ドライブより前にある場合、そのコンピュータは USB フラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

1. コンピュータの電源を切ります。
2. USB フラッシュ メディア デバイスをコンピュータの USB ポートのどれかに差し込み、USB ディスケット ドライブ以外のすべての USB ストレージ デバイスを取り外します。
3. FDISK.COM と、SYS.COM または FORMAT.COM のどちらかが格納された起動可能な DOS ディスケットをディスケット ドライブに挿入します。コンピュータの電源を入れて、DOS ディスケットを起動します。
4. **A:**プロンプトで「FDISK」と入力して[Enter]キーを押し、FDISK を実行します。メッセージが表示されたら、**[Yes]**（Y）をクリックして大容量ディスクのサポートを有効にします。
5. 選択肢の「5」を入力してコンピュータのドライブを表示します。一覧のドライブの中で最も容量が近いドライブが USB メモリで、通常は一覧の最後に表示されます。ドライブ名を書き留めておきます。

   USB メモリのドライブ名：__________

   △ **注意：** ドライブが USB メモリと一致しない場合は、データの損失を防ぐため、次の手順に進まないでください。他にストレージ デバイスがないか、すべての USB ポートを確認します。あった場合は取り外してコンピュータを再起動し、手順 4 に進みます。ない場合、コンピュータが USB メモリに対応していないか、USB メモリが破損しています。この場合は USB メモリを起動可能にするための手順を実行しないでください。

6. Esc キーを押して **A:**プロンプトに戻り、FDISK を終了します。
7. 起動可能な DOS ディスケットに SYS.COM がある場合は手順 8 に、ない場合は手順 9 に進みます。
8. **A:**プロンプトで、「SYS x:」（x は書き留めたドライブ名）と入力します。

   △ **注意：** USB メモリのドライブ名を正しく入力したことを確認します。

   システム ファイルの転送が完了すると、SYS から **A:**プロンプトに戻ります。手順 13 に進みます。

9. 保存しておきたいファイルを USB メモリから別のドライブ（コンピュータの内蔵ハードディスク ドライブなど）の一時ディレクトリにコピーします。

10. **A:**プロンプトで、「FORMAT /S X:」（X は書き留めたドライブ名）と入力します。

△ **注意：** USB メモリのドライブ名を正しく入力したことを確認します。

FORMAT では 1 つ以上の警告が表示され、次の手順に進む前に毎回確認画面が表示されます。毎回「Y」と入力します。FORMAT により USB メモリがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。

11. ラベルを付けない場合は Enter キーを押し、必要な場合はラベルを入力します。

12. 手順 9 でコピーしたファイルを USB メモリにコピーしなおします。

13. ディスケットを取り出し、コンピュータを再起動します。USB フラッシュ メディア デバイスが C ドライブとして起動されます。

注記： 初期設定の起動順序はコンピュータによって異なり、コンピュータ セットアップ（F10）ユーティリティで変更することができます。

Windows 9x から DOS バージョンを使用した場合、短い間 Windows ロゴの画面が表示されることがあります。表示されないようにするには、USB フラッシュ メディア デバイスのルート ディレクトリに LOGO.SYS というゼロ長のファイルを追加します。

「18 ページの 「複数のコンピュータへのコピー」」に戻ります。

サポートされない USB フラッシュ メディア デバイス

起動可能な USB フラッシュ メディア デバイスを作成するには、次のものが必要です。

- USB フラッシュ メディア デバイス
- FDISK および SYS プログラムが格納された、起動可能な DOS ディスケット（SYS がない場合は FORMAT を使用できますが、USB メモリ上のファイルがすべて失われます）
- USB フラッシュ メディア デバイスから起動可能なコンピュータ

△ **注意：** 一部の古いコンピュータでは、USB フラッシュ メディア デバイスから起動できない場合があります。コンピュータ セットアップ（F10）ユーティリティに表示される初期設定の起動順序で、USB デバイスがハードディスク ドライブより前にある場合、そのコンピュータは USB フラッシュ メディア デバイスから起動できます。それ以外の場合は、起動可能ディスケットを使用してください。

1. SCSI、ATA RAID、または SATA ドライブが取り付けられた PCI カードがコンピュータにある場合は、コンピュータの電源を切って電源コードを抜き取ります。

△ **注意：** 電源コードは必ず抜き取ってください。

2. コンピュータのカバーを開いて PCI カードを取り外します。

3. USB フラッシュ メディア デバイスをコンピュータの USB ポートのどれかに差し込み、USB ディスケット ドライブ以外のすべての USB ストレージ デバイスを取り外します。コンピュータのカバーを閉じます。

4. 電源コードを差し込んでコンピュータの電源を入れます。

5. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。

6. **[カスタム]**（Advanced）→**[PCI デバイス]**（PCI Devices）の順に選択して PATA および SATA コントローラを無効にします。SATA コントローラを無効にするとき、コントローラに割り当てられている IRQ を書き留めておきます。後で再び IRQ を割り当てる必要があります。変更を確定して、セットアップ ユーティリティを終了します。

   SATA IRQ : __________

7. FDISK.COM と、SYS.COM または FORMAT.COM のどちらかが格納された起動可能な DOS ディスケットをディスケット ドライブに挿入します。コンピュータの電源を入れて、DOS ディスケットを起動します。

8. FDISK を実行して USB フラッシュ メディア デバイス上にあるパーティションをすべて削除します。新しいパーティションを作成して有効にします。Esc キーを押して FDISK を終了します。

9. FDISK を終了してもコンピュータが自動的に再起動されない場合は、Ctrl ＋ Alt ＋ Del キーを押して、DOS ディスケットから起動しなおします。

10. **A:**プロンプトで「FORMAT C: /S」と入力し、Enter キーを押します。FORMAT により USB フラッシュ メディア デバイスがフォーマットされ、システム ファイルが追加され、ボリューム ラベルが要求されます。

11. ラベルを付けない場合は Enter キーを押し、必要な場合はラベルを入力します。

12. コンピュータの電源を切って電源コードを抜き取ります。コンピュータのカバーを開き、取り外しておいた PCI カードを取り付けなおします。コンピュータのカバーを閉じます。

13. 電源コードを差し込み、ディスケットを取り出してコンピュータの電源を入れます。

14. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

15. **[カスタム]**→**[PCI デバイス]**の順に選択して、手順 6 で無効にした PATA および SATA コントローラを再び有効にします。SATA コントローラを元の IRQ に割り当てなおします。

16. 変更を保存してユーティリティを終了します。USB フラッシュ メディア デバイスが C ドライブとして起動されます。

注記： 初期設定の起動順序はコンピュータによって異なり、コンピュータ セットアップ（F10）ユーティリティで変更することができます。手順については、Documentation and Diagnostics CD（ドキュメンテーションおよび診断ユーティリティ CD）に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。

Windows 9x から DOS バージョンを使用した場合、短い間 Windows ロゴの画面が表示されることがあります。表示されないようにするには、USB フラッシュ メディア デバイスのルート ディレクトリに LOGO.SYS というゼロ長のファイルを追加します。

「18 ページの 「複数のコンピュータへのコピー」」に戻ります。

8 電源ボタン

お使いのコンピュータで ACPI（Advanced Configuration and Power Interface）を使用している場合は、電源ボタンをコンピュータのオン/オフ スイッチとしての機能のほか、スタンバイ モードを起動するためのボタンとして設定することができます。スタンバイ モードでは、電源を完全に切らずに、コンピュータの消費電力を低い状態に保つことができます。使用中のアプリケーションを終了せずに作業を途中で中断したい場合など、スタンバイ モードに設定しておくとコンピュータの電力を低く抑えることができます。

電源ボタンの設定を変更するには、以下の手順で操作します。

1. **[スタート]**ボタンをクリックし、**[コントロール パネル]**→**[パフォーマンスとメンテナンス]**→**[電源オプション]**の順に選択します。
2. **[電源オプションのプロパティ]**で**[詳細設定]**タブを選択します。
3. **[電源ボタン]**で**[スタンバイ]**を選択します。

電源ボタンにスタンバイ ボタンとしての機能を設定してある場合は、コンピュータの電源が入っているときに電源ボタンを押すと、スタンバイ モードを起動することができます。再び電源ボタンを押すと、直ちにスタンバイ モードから復帰できます。コンピュータの電源を完全に切るには、電源ボタンを 4 秒以上押し続けます。

△ **注意：** システムが応答しない場合以外は、電源ボタンを使って電源を切らないでください。オペレーティング システムを通さずに電源を切ると、ハードディスク ドライブが破損したりデータが損失したりする可能性があります。

9 HP Web サイト サポート

HP では自社製のソフトウェアのテストおよび修正を行い、オペレーティング システムに特化したサポート ソフトウェアを開発しています。このため、HP のコンピュータは優れた性能、互換性、および信頼性を兼ね備えています。

別の種類のオペレーティング システムをインストールしたり新しいバージョンのオペレーティング システムに移行したりする場合、それぞれのオペレーティング システム用に設計されたサポート ソフトウェアを実行してください。お使いのコンピュータにインストールされているバージョンと異なるバージョンの Microsoft Windows を実行したい場合、対応するデバイス ドライバおよびユーティリティをインストールして、すべての機能がサポートされ、正しく動作することを確認してください。

HP では、最新版のサポート ソフトウェアの検索、ダウンロード、インストールなどをより簡単に行えるようにしていきます。ソフトウェアは http://www.hp.com/support/からダウンロードできます。

HP のホームページには、HP 製のコンピュータで Microsoft Windows のオペレーティング システムを実行する際に必要な最新のデバイス ドライバ、ユーティリティ、フラッシュ ROM イメージなどが用意されています。

10 業界標準

HP のインテリジェント マネジメント機能は、各社のシステム マネジメント アプリケーションを取り入れており、次のようなコンピュータ業界の標準規格に準拠しています。

- Web-Based Enterprise Management（WBEM）
- Windows Management Interface（WMI）
- Wake on LAN テクノロジ
- ACPI
- SMBIOS
- Pre-boot Execution（PXE）サポート

11 資産情報管理機能およびセキュリティ機能

コンピュータに搭載される資産情報管理機能を使用すれば、HP Systems Insight Manager、HP Client Manager、HP OpenView PC Configuration Management Solution、OpenView Client Configuration Manager、および Asset Management ソリューション（Windows Vista では現在使用不可）、またはその他のシステム管理アプリケーションを使用して管理される資産情報を確認することができます。資産情報管理機能とこれらの管理ソフトウェア製品を統合することにより、お使いの環境に最適な管理ソフトウェアを選択でき、今までお使いになっていたソフトウェアをより有効に活用できます。

さらに、HP では、コンピュータとデータを不正なアクセスから保護するための機能を備えています。HP Embedded Security for ProtectTools がインストールされている場合は、データへの不正なアクセスの防止、システムの整合性の確認、および第三者からのアクセスに対する認証が行われます。（詳しくは、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャ ガイド』を参照してください。）一部のモデルに装備されている HP Embedded Security for ProtectTools、スマート カバー センサ（Smart Cover Sensor）、スマート カバー ロック（Smart Cover Lock）などのセキュリティ機能は、パーソナル コンピュータの内部装置への不正なアクセスの防止に役立ちます。パラレル ポート、シリアル ポート、または USB ポートを無効にすることにより、またリムーバブル メディア ブート機能を無効にすることにより、貴重な資産であるデータを保護できます。これ以外にも、メモリ脱着センサおよびスマート カバー センサ/カバー リムーバル センサからの警告が自動的にシステム管理アプリケーションに転送されることで、コンピュータの内部装置への不正なアクセスを防ぐことができます。

注記： HP Embedded Security for ProtectTools、スマート カバー センサ/カバー リムーバル センサ、およびスマート カバー ロックは、一部のシステムにオプションとして装備されています。

次のユーティリティを使用して、セキュリティ機能の設定を管理できます。

- コンピュータ セットアップ（F10）ユーティリティを使用してローカルで管理します。コンピュータ セットアップ（F10）ユーティリティの詳しい情報と手順については、コンピュータに付属の Documentation and Diagnostics CD に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。また、コンピュータによっては HP BIOS Configuration for ProtectTools が含まれています。これは、ProtectTools の Windows ベースのコンポーネントで、管理者が動作中の OS 内から BIOS のセキュリティ設定を行うことができます。
- HP Client Manager Software、OpenView Client Configuration Manager、または System Software Manager を使用してリモートで管理します。このソフトウェアにより、ネットワークのセキュリティ機能の設定を確実に、一貫して集中管理することができます。

次の表と各項で、コンピュータ セットアップ（F10）ユーティリティを使ってローカルでコンピュータのセキュリティ機能を管理する方法を説明します。

表 11-1 セキュリティ機能

項目	説明
セットアップ パスワード（Setup Password）	セットアップ（管理者）パスワードを設定して有効にします

表 11-1 セキュリティ機能 (続き)

項目	説明
	注記： セットアップ パスワードを設定すると、コンピュータ セットアップ（F10）ユーティリティの設定を変更したり、ROM をフラッシュしたり、Windows 環境で特定のプラグ アンド プレイ設定を変更したりする場合にセットアップ パスワードが必要になります 詳しくは、Documentation and Diagnostics CD に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください
電源投入時パスワード（Power-On Password）	電源投入時パスワードを設定して有効にします 詳しくは、Documentation and Diagnostics CD に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください
パスワード オプション（Password Options） （電源投入時パスワードが設定されている場合にのみ表示されます）	ウォーム ブート（Ctrl + Alt + Del）にパスワードが必要かどうかを指定します 詳しくは、Documentation and Diagnostics CD に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください
起動前の承認（Pre-Boot Authorization）	電源投入時パスワード（Power-On Password）の代わりにスマート カードを使用する設定を有効/無効にします
スマート カバー（Smart Cover）	次の項目を設定します ● カバー ロック（Cover Lock）の有効（Enable）/無効（Disable）の設定 ● カバー リムーバル センサの有効/無効の設定 **注記：** **[ユーザに通知]**を設定すると、カバーが取り外されたことをセンサが検知したときにユーザに通知されます。セットアップ パスワードは、カバーが取り外されたことをセンサが検知した場合、コンピュータを起動する際にセットアップ パスワードの入力を要求します 一部のモデルでのみサポートされます。詳しくは、Documentation and Diagnostics CD に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください
内蔵セキュリティ（Embedded Security）	次の項目を設定します ● 内蔵セキュリティ デバイスの有効（Enable）/無効（Disable） ● デバイスの出荷時設定へのリセット 一部のモデルでのみサポートされます。http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャ ガイド』を参照してください
デバイス セキュリティ（Device Security）	シリアル ポート（Serial Port）、パラレル ポート（Parallel Port）、前面の USB ポート（Front USB Port）、オーディオ セキュリティ（Audio Security）、モデルによってはネットワーク コントローラ（Network Controller）、および SCSI コントローラ（SCSI Controller）のデバイス有効（Enable）/デバイス無効（Disable）を設定します
ネットワーク サービス ブート（Network Service Boot）	ネットワーク サーバにインストールされたオペレーティング システムからコンピュータを起動する機能を有効（Enable）または無効（Disable）にします （ネットワーク コントローラが PCI バス上に存在するか、システム ボードに組み込まれている必要があります）
システム ID（System ID）	次の項目を設定します ● アセット タグ（Asset Tag。18 バイトの ID）およびオーナーシップ タグ（Ownership Tag。POST 実行中に表示される 80 バイトの ID）の入力 詳しくは、Documentation and Diagnostics CD に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください ● 本体シリアル番号（Chassis Serial Number）または UUID（Universal Unique Identifier）の入力 UUID は現在の本体シリアル番号が無効の場

表 11-1 セキュリティ機能 (続き)

項目	説明
	合にのみ更新できます（通常これらの識別（ID）番号は工場出荷時に設定され、そのシステムを特定するために使用されます） キーボード（Keyboard Locale）の設定：英語用やドイツ語用などをシステム ID エントリに対して設定します
ドライブロック（DriveLock）（一部のモデルのみ）	ATA ハードディスク ドライブにマスタ パスワードまたはユーザ パスワードを割り当てたり、パスワードを変更したりします。この機能が有効の場合は、POST 実行中にどちらかの DriveLock パスワードを入力するよう求められます。どちらのパスワードも正常に入力されなかった場合は、次のコールド ブート シーケンスの間にどちらかのパスワードが入力されるまで、ハードディスク ドライブにはアクセスできません 注記：　この項目は、ATA Security コマンド セットをサポートする ATA ハードディスク ドライブが少なくとも 1 台システムに接続されている場合にのみ表示されます 詳しくは、Documentation and Diagnostics CD に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください
コンピュータ セットアップ（F10）ユーティリティについて詳しくは、Documentation and Diagnostics CD に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。 サポートされるセキュリティ機能は、お使いのコンピュータの構成によって異なる場合があります。	

パスワードのセキュリティ

電源投入時パスワード（Power-on password）を設定すると、コンピュータの電源を入れたり再起動したりするたびに、アプリケーションやデータにアクセスするためのパスワードの入力が要求されるので、コンピュータが許可無く使用されることを防止できます。セットアップ パスワード（Setup password）は、特にコンピュータ セットアップ（F10）ユーティリティへの不正アクセスを防ぎます。セットアップ パスワードを、電源投入時パスワードの補助手段として使用することもできます。つまり、電源投入時パスワードの入力を要求されたときに、代わりにセットアップ パスワードを入力してコンピュータにアクセスすることもできます。

ネットワーク全体のセットアップ パスワードを設定しておくと、システム管理者はネットワーク上のすべてのシステムにログインでき、設定されている電源投入時パスワードを知らなくてもメンテナンスを行うことができます。

セットアップ パスワードの設定

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャ ガイド』を参照してください。**[コンピュータ セットアップ（F10）ユーティリティ]**メニューで、セットアップ パスワードを設定しておけば、無断でコンピュータが再設定されることを防止できます。

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。

2. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

注記：　適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。

3. **[セキュリティ]**（Security）→**[セットアップ パスワード]**（Setup Password）の順に選択した後、画面上のメッセージに従って操作します。

4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

電源投入時パスワードの設定

[コンピュータ セットアップ ユーティリティ]メニューで、電源投入時パスワードを設定しておけば、無断でコンピュータが使用されることを防止できます。電源投入時パスワードが設定されていると、コンピュータ セットアップ ユーティリティの**[セキュリティ設定]**（Security）メニューに**[パスワード オプション]**（Password Options）が表示されます。パスワード オプションには**[ウォーム ブート時のパスワード入力]**（Password Prompt on Warm Boot）などが含まれます。**[ウォーム ブート時のパスワード入力]**が有効にされている場合も、コンピュータを再起動するたびにパスワードを入力する必要があります。

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。

2. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。

3. **[セキュリティ]**（Security）→**[電源投入時パスワード]**（Power-On Password）の順に選択した後、画面上のメッセージに従って操作します。

4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

電源投入時パスワードの入力

電源投入時パスワードを入力するには、以下の手順で操作します。

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。

2. 鍵形のアイコンが表示されたら、パスワードを入力して Enter キーを押します。

注記： 機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、鍵形に×印のついたアイコンが表示されますので、再度試してください。続けて 3 回間違えた場合は、コンピュータの電源をいったん切って最初から操作しなおす必要があります。

セットアップ パスワードの入力

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャ ガイド』を参照してください。

コンピュータでセットアップ パスワードを設定しておけば、**[コンピュータ セットアップ ユーティリティ]**メニューを実行するたびに、必ずパスワードの入力が必要となります。

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。
2. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。

3. 鍵形のアイコンが表示されたら、セットアップ パスワードを入力して Enter キーを押します。

   注記： 機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

間違ったパスワードを入力した場合は、鍵形に×印のついたアイコンが表示されますので、パスワードを正しく入力しなおしてください。続けて 3 回間違えた場合は、コンピュータの電源をいったん切って最初から操作しなおす必要があります。

電源投入時パスワードまたはセットアップ パスワードの変更

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャ ガイド』を参照してください。

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**[再起動]**の順に選択します。
2. 電源投入時パスワードを変更する場合は、手順 3 に進みます。

   セットアップ パスワードを変更する場合は、コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。

3. 鍵形のアイコンが表示されたら、次のように入力します。現在のパスワード/新しいパスワード/新しいパスワード

   注記： 機密保護のため、入力したパスワードは画面に表示されません。パスワードを入力する際は、間違えないよう注意してください。

4. Enter キーを押します。

新しいパスワードは、次にコンピュータの電源を入れたときから有効になります。

注記： 代替の区切り文字について詳しくは、「30 ページの 「各国語キーボードの区切り文字」」を参照してください。電源投入時パスワードとセットアップ パスワードは、コンピュータ セットアップ（F10）ユーティリティの**[セキュリティ]**（Security）オプションを使って変更することもできます。

電源投入時パスワードまたはセットアップ パスワードの削除

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャ ガイド』を参照してください。

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]**→**[シャットダウン]**→**再起動**の順に選択します。
2. 電源投入時パスワードを削除する場合は、手順 3 に進みます。

   セットアップ パスワードを削除する場合は、コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記：　適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。

3. 鍵形のアイコンが表示されたら、次のように入力します。現在のパスワード/
4. Enter キーを押します。

   注記：　代替の区切り文字について詳しくは、「30 ページの 「各国語キーボードの区切り文字」」を参照してください。電源投入時パスワードとセットアップ パスワードは、コンピュータ セットアップ（F10）ユーティリティの**[セキュリティ]**（Security）オプションを使って変更することもできます。

各国語キーボードの区切り文字

各キーボードは各国固有の要件に合うように設計されています。パスワードの変更または削除に使用する構文およびキーは、コンピュータに付属するキーボードによって異なります。

各国語キーボードの区切り文字					
/	アラビア語圏	-	ギリシャ	/	ロシア
=	ベルギー	.	ヘブライ語圏	-	スロバキア
-	BHCSY*	-	ハンガリー	-	スペイン
/	ブラジル	-	イタリア	/	スウェーデン/フィンランド
/	中国	/	日本	-	スイス
-	チェコ	/	韓国	/	台湾
-	デンマーク	-	中南米	/	タイ
!	フランス	-	ノルウェー	.	トルコ
é	カナダ（フランス語圏）	-	ポーランド	/	米国
-	ドイツ	-	ポルトガル		
	* ボスニア ヘルツェゴビナ、クロアチア、スロベニア、ユーゴスラビア				

電源投入時パスワードを忘れてしまった場合

設定しておいた電源投入時パスワードを忘れると、コンピュータを使用できなくなります。パスワードを解除する方法については、Documentation and Diagnostics CD に収録されている『トラブルシューティング ガイド』を参照してください。

システムに内蔵セキュリティ デバイスが搭載されている場合は、http://www.hp.com/jp/から入手できる『HP ProtectTools セキュリティ マネージャ ガイド』を参照してください。

ドライブロック（DriveLock）

ドライブロックは、ATA ハードディスク ドライブにあるデータへの不正アクセスを防止する業界標準のセキュリティ機能です。コンピュータ セットアップ（F10）ユーティリティの拡張機能として実装されています。この機能は、ATA Security コマンド セットに対応するハードディスク ドライブが検出された場合にのみ利用できます。ドライブロックは、データのセキュリティを最重要視するユーザ向けに開発されました。このようなユーザにとっては、ハードディスク ドライブのコストとそこに格納されているデータの喪失は、データへの不正アクセスの結果生じる可能性のある損害に比べれば、些細なものです。このレベルのセキュリティの確保と同時に、パスワードを忘れたときの対処もできるように、HP が実装したドライブロックでは、2 つのパスワードによるセキュリティ方式を採用しています。一方のパスワードはシステム管理者が設定して使用するもので、もう一方のパスワードは通常、エンド ユーザが設定して使用します。両方のパスワードを忘れてしまった場合にドライブをアンロックするための手段はありません。したがって、ハードディスク ドライブに含まれるデータが企業情報システムに複製されているか、または定期的にバックアップが作成されている場合に、ドライブロックを最も安全に使用できます。ドライブロックの両方のパスワードを忘れてしまった場合は、ハードディスク ドライブを使用できなくなります。前に述べたカスタマ プロファイルに適合しないすべてのユーザにとって、この事実は受け入れ難いリスクになる可能性があります。一方、カスタマ プロファイルに適合するユーザにとっては、ハードディスク ドライブに保存されたデータの性質上、許容できるリスクだと言えます。

ドライブロックの使用法

ATA Security コマンド セットに対応するハードディスク ドライブが 1 つ以上検出された場合、**[ドライブロック]**（DriveLock）オプションは、コンピュータ セットアップ（F10）ユーティリティの**[セキュリティ]**（Security）メニューに表示されます。ユーザには、マスタ パスワード（master password）を設定したりドライブロックを有効にしたりするオプションが提供されます。ドライブロックを有効にするには、ユーザ パスワード（user password）を入力する必要があります。通常、ドライブロックの最初のコンフィギュレーションはシステム管理者が実行するので、マスタ パスワードを最初に設定する必要があります。ドライブロックを有効にするか無効のままにしておくかにかかわらず、管理者はマスタ パスワードを設定することをおすすめします。これにより、将来ドライブがロックされた場合に、管理者はドライブロックの設定値を変更できるようになります。マスタ パスワードが設定されると、システム管理者はいつでもドライブロックを有効にしたり無効にしたりすることができます。

ロックされたハードディスク ドライブが存在する場合は、POST（Power-On Self Test）によって、そのドライブをアンロックするためのパスワードが要求されます。電源投入時パスワード（power-on password）が設定されていて、そのドライブのユーザ パスワードと一致する場合は、パスワードの再入力は要求されません。一致しない場合は、ドライブロックのパスワードを入力するよう要求されます。コールド ブート時には、マスタ パスワードとユーザ パスワードのどちらも使うことができます。ウォーム ブート時には、コールド ブートの前にドライブのロック解除に使用したパスワードと同じものを入力します。ユーザは、パスワードが正しいと認識されるまで、2 回入力できます。コールド ブート時には、2 回とも間違えた場合でも POST は続行されますが、そのドライブにはアクセスできません。ウォーム ブート時または Windows からの再起動時には、2 回とも間違えた場合は POST が停止され、再起動するよう求められます。

ドライブロックの使用例

ドライブロックのセキュリティ機能は、企業環境での使用に最も適しています。システム管理者はハードディスク ドライブのコンフィギュレーションを担当しますが、その作業には、ドライブロックのマスタ パスワードおよび一時ユーザ パスワードを設定することが含まれます。ユーザがユーザ パスワードを忘れた場合や、コンピュータを別の従業員が使うことになった場合、システム管理者はマスタ パスワードを使用して、ユーザ パスワードをリセットしたり、ハードディスク ドライブへのアクセス権を回復したりすることができます。

企業システム管理者は、ドライブロックを有効にする場合、マスタ パスワードの設定とメンテナンスについての企業方針を確立しておくことをおすすめします。これは、従業員が会社を辞める前に意図的に、または誤ってドライブロックの両方のパスワードを設定してしまうという状況を防ぐために必要です。両方のパスワードを設定した従業員が会社を辞めてしまった場合、そのハードディスク ドライブは使用不能となり、交換が必要になります。また、マスタ パスワードが設定されていないと、システム管理者がロックされたハードディスク ドライブにアクセスできなくなり、不正ソフトウェアの日常チェックや、その他の資産管理およびサポートを実行できなくなることがあります。

それほど厳重なセキュリティを必要としないユーザの場合は、ドライブロックを有効にしないことをおすすめします。この種のユーザには、個人ユーザや、機密性の高いデータをハードディスク ドライブに保持しないことを習慣にしているユーザが含まれます。このようなユーザにとっては、両方のパスワードを忘れてハードディスク ドライブが使えなくなることのほうが、ドライブロックにより保護されるデータの価値よりもはるかに大きな問題と言えます。コンピュータ セットアップ（F10）ユーティリティとドライブロックへのアクセスは、セットアップ パスワードによって制限できます。セットアップ パスワードを指定してそれをエンド ユーザに公表しないことで、システム管理者はユーザがドライブロックを有効にできないようにします。

スマート カバー センサ/カバー リムーバル センサ（Cover Removal Sensor）

一部のモデルに搭載されているスマート カバー センサ/カバー リムーバル センサとは、本体のカバーまたはサイド パネルの着脱があったことをユーザに知らせる、ハードウェア技術とソフトウェア技術を結合した機能です。3 段階の設定レベルがあり、本体のカバーの着脱があった後で初めてコンピュータの電源を入れたときの動作が異なります。

表 11-2 スマート カバー センサ/カバー リムーバル センサの動作

レベル	設定	説明
レベル 0	無効（Disabled）	スマート カバー センサ/カバー リムーバル センサは無効（初期設定）
レベル 1	ユーザに通知（Notify User）	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される
レベル 2	セットアップ パスワード（Setup Password）	本体のカバーが取り外されたことを知らせるメッセージが画面に表示される。セットアップ パスワードを入力するまで、コンピュータを使用できない

注記： これらの設定は、コンピュータ セットアップを使用して変更できます。コンピュータ セットアップ（F10）ユーティリティについて詳しくは、Documentation and Diagnostics CD に収録されている『コンピュータ セットアップ（F10）ユーティリティ ガイド』を参照してください。

スマート カバー センサ/カバー リムーバル センサ（Cover Removal Sensor）の保護レベルの設定

スマート カバー センサ/カバー リムーバル センサ機能を有効に設定するには、以下の手順で操作します。

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]→[シャットダウン]→[再起動]**の順に選択します。
2. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。
3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）→**[カバー リムーバル センサ]**（Cover Removal Sensor）の順に選択した後、必要なセキュリティ レベルを選択します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

スマート カバー ロック

スマート カバー ロックは、コンピュータのカバーのロックをソフトウェアで制御する、一部の HP のコンピュータでサポートされる機能です。このロックによって、承認されていないユーザによるコンピュータ内部のコンポーネントへの不正なアクセスを防ぐことができます。工場出荷時には、ロックが解除された状態になっています。

注意： カバー ロック セキュリティを最大限にするために、必ずセットアップ パスワードを設定してください。セットアップ パスワードによって、コンピュータ セットアップ（F10）ユーティリティへの不正なアクセスを防止できます。

注記： スマート カバー ロックは、一部のシステムにオプションとして装備されています。

スマート カバー ロックの設定

スマート カバー ロックを使ってコンピュータ本体のカバーをロックするには、以下の手順で操作します。

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]→[シャットダウン]→[再起動]**の順に選択します。
2. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。

3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）→**[カバー ロック]**（Cover Lock）→**[ロック]**（Lock）の順に選択します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

スマート カバー ロックの解除

1. コンピュータの電源を入れるか再起動します。Microsoft Windows をお使いの場合は、**[スタート]→[シャットダウン]→[再起動]**の順に選択します。
2. コンピュータが起動してモニタ ランプが緑色に点灯したらすぐに F10 キーを押し、コンピュータ セットアップ（F10）ユーティリティを実行します。必要であれば、Enter キーを押すと、タイトル画面をスキップできます。

   注記： 適切なタイミングで F10 キーを押せなかった場合は、コンピュータを再起動して、モニタ ランプが緑色に点灯したときにもう一度 F10 キーを押します。

3. **[セキュリティ]**（Security）→**[スマート カバー]**（Smart Cover）→**[カバー ロック]**（Cover Lock）→**[アンロック]**（Unlock）の順に選択します。
4. 設定を終了するには、**[ファイル]**（File）→**[変更を保存して終了]**（Save Changes and Exit）の順に選択します。

Smart Cover FailSafe キーの使用

スマート カバー ロックを使ってコンピュータをロックしたまま、パスワードを入力できなくなってしまった場合、Smart Cover FailSafe キーを使用して、コンピュータ本体のカバーを開ける必要があります。Smart Cover FailSafe キーは、次のような場合に必要となります。

- 停電
- 起動障害
- コンピュータ部品（プロセッサや電源など）の障害
- パスワードを忘れてしまった場合

△ 注意： Smart Cover FailSafe キーは、HP が提供する専用ツールです。このキーが必要になる前に、HP 製品販売店であらかじめご用意いただくことをおすすめします。

FailSafe キーは次の方法で入手できます。

- HP のサポート窓口に問い合わせます。
- 保証規定に記載されている適切な番号に連絡します。

Smart Cover FailSafe キーについて詳しくは、Documentation and Diagnostics CD に収録されている『ハードウェア リファレンス ガイド』を参照してください。

ケーブル ロックの取り付け

コンピュータのリア パネルにはケーブル ロックを取り付けられるようになっているので、市販のケーブル ロックを使用して、コンピュータを作業エリアに固定できます。

詳しくは、Documentation and Diagnostics CD に収録されている『ハードウェア リファレンス ガイド』を参照してください。

指紋認証テクノロジ

HP 指紋認証テクノロジを使用すると、エンド ユーザのパスワードの入力が不要となるため、ネットワークのセキュリティを強化する一方で、ログイン手順を簡素化し、企業のネットワーク管理に関わる経費を削減することができます。また、手頃な価格のため、もはや一部のハイテク産業や高度なセキュリティを扱う組織や企業だけのものではなくなりました。

注記： モデルによっては、指紋認証テクノロジがサポートされていない場合があります。

詳しくは、次の Web サイト（英語サイト）を参照してください。

http://h18004.www1.hp.com/products/security/

障害通知および復旧機能

障害通知および復旧機能とは、最新のハードウェア/ソフトウェア技術を結合して、重要なデータの損失を防ぎ、故障時間を最小限に抑える機能です。

HP Client Manager によって管理されるネットワークにコンピュータが接続されている場合、ネットワーク管理ソフトウェアに障害通知が送られます。HP Client Manager Software では、管理されているすべてのコンピュータで診断ユーティリティを実行し、失敗したテストの概要を作成するよう、リモートでスケジュールを設定することもできます。

ドライブ保護システム

ドライブ保護システム（DPS）は、一部のモデルに搭載されたハードディスク ドライブに組み込まれている診断ツールです。DPS を使用して、保証規定が適用されない、ハードディスク ドライブの交換に至るような問題を診断します。

コンピュータの組み立て時に各ハードディスク ドライブに対して DPS テストが実行され、主要な情報がハードディスク ドライブに書き込まれます。この情報は半永久的に記録されます。DPS が実行されるたびに、テストの結果がハードディスク ドライブに書き込まれます。サポート窓口では、この情報をもとに、DPS ソフトウェアを実行する原因となった状況を特定することができます。DPS の使用方法については、Documentation and Diagnostics CD に収録されている『トラブルシューティング ガイド』を参照してください。

耐サージ機能付連続供給電源装置

耐サージ機能が付いた連続供給電源によって、急激な電圧の変化に対処することができます。この電源装置は、データの損失やシステム ダウンを引き起こさずに 2000 V までのサージ電圧に耐えられることが確認されています。

温度センサ機能

温度センサ機能は、ハードウェアとソフトウェアの統合により提供される機能で、コンピュータ内部の温度を監視します。温度が通常の範囲を超えると、画面上に警告メッセージが表示されるため、内部部品の故障やデータの損失が発生する前に対処することができます。

索引